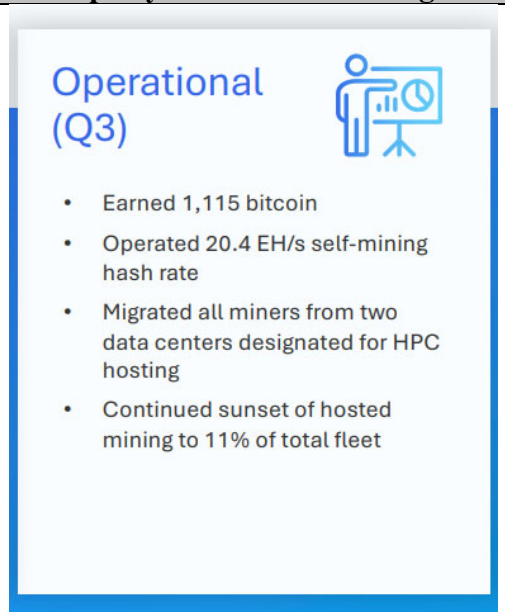
Exhibit 7

Exhibit 9: U.S. Patent No. 10,284,370

Claim 1	CExemplary Evidence of Infringement
1[pre] A method performed by a hardware processor of a computing device, comprising:	Core Scientific, Inc. (hereinafter "Core") performs a method using a hardware processor of a computing device. For example, Core verifies Bitcoin transactions. *See*, *e.g.*: "Core Scientific, Inc. is a leader in digital infrastructure for bitcoin mining and high-performance computing. We operate dedicated, purpose-built facilities for digital asset mining and are a premier provider of digital infrastructure, software solutions and services to our third-party customers. We employ are own large fleet of computers ('miners') to earn digital assets for our own account and we provide hosting services for large bitcoin mining customers …. We derive the majority of our revenue from earning bitcoin for our own account ('self-mining')." *See*, *e.g.*, Core Scientific., Inc., Quarterly report pursuant to Section 13 and 15(d), (Form 10-Q), at Note 1, filed Nov. 06, 2024, available at https://www.sec.gov/ix?doc=/Archives/edgar/data/1839341/000162828024045811/core-20240930.htm "We currently operate in three segments: 'Digital Asset Self-Mining' consisting of digital asset mining for our own account, 'Digital Asset Hosted Mining' consisting of our digital infrastructure and third-party hosting services for digital asset mining, and 'HPC Hosting' consisting of our digital infrastructure and third-party hosting services for client HPC operations. Prior to April 1, 2024, we operated only in the Digital Asset Self-Mining and Digital Asset Hosted Mining segments." *See*, *e.g.*, Core Scientific., Inc., Quarterly report pursuant to Section 13 and 15(d), (Form 10-Q), at Note 1, filed Nov. 06, 2024, available at https://www.sec.gov/ix?doc=/Archives/edgar/data/1839341/000162828024045811/core-20240930.htm For example, Core earned 1,115 Bitcoin in Q3, 2024 from self-mining activities, operating with 20.4 EH/s self-mining hash rate. *See*, *e.g.*:

Claim 1	CExemplary Evidence of Infringement



See, *e.g.*, Core Scientific, Third Quarter Fiscal 2024 Earnings Presentation, Nov. 6, 2024, at 6, available at https://d1io3yog0oux5.cloudfront.net/_af714ff3677136aff8992204fdbd0bc5/corescientific/db/946/9319/presentation/Core+Scientific+Q3+2024+Earnings+Presentation.pdf

"**Bitcoin signed messages have three parts, which are the Message, Address, and Signature**. The message is the actual message text - all kinds of text is supported, but it is recommended to avoid using non-ASCII characters in the signature because they might be encoded in different character sets, preventing signature verification from succeeding.

The address is a legacy, nested segwit, or native segwit address. Message signing from legacy addresses was added by Satoshi himself and therefore does not have a BIP. **Message signing from segwit addresses has been added by BIP137 … The Signature is a base64-encoded ECDSA signature** that, when decoded, with fields described in the next section." (Emphasis added)

Claim 1	CExemplary Evidence of Infringement
	See, *e.g.,* Message Signing, https://en.bitcoin.it/wiki/Message_signing. "This document describes a signature format for **signing messages with Bitcoin private keys**. The specification is intended to describe the standard for signatures of messages that can be signed and verified between different clients that exist in the field today." (Emphasis added) *See*, *e.g.*, Bitcoin BIP137, https://github.com/bitcoin/bips/blob/master/bip-0137.mediawiki. For example, Core utilizes a computer (*e.g.*, a node, a miner, etc.) comprising one or more processors (*e.g.*, ASIC, GPUs, etc.). *See*, *e.g.*: "Bitcoin is a decentralized digital currency that enables instant payments to anyone, anywhere in the world. Bitcoin uses peer-to-peer technology to operate with no central authority: transaction management and money issuance are carried out collectively by the network." *See*, *e.g.*, Welcome to the Bitcoin Wiki, https://en.bitcoin.it/wiki/Main_Page. Full nodes are the ones that really support and secure the Bitcoin blockchain, and they are indispensable to the network. Full nodes (or fully validating nodes) are responsible for verifying transactions and blocks according to the rules of the Bitcoin protocol. And since the network is distributed, the rules are enforced by Bitcoin's consensus algorithm. *See*, *e.g.*, Node, https://academy.binance.com/en/glossary/node.

Claim 1	CExemplary Evidence of Infringement

> In the world of cryptocurrencies, the term ASIC is widely used to refer to the specialized hardware that are being developed and regularly improved by companies such as Bitmain and Halong Mining. These hardware are designed with the sole intention of mining Bitcoin (or other cryptocurrencies). There are some coins that cannot be effectively mined using ASIC miners and, as such, may be referred to as ASIC-resistant cryptocurrencies.

See, *e.g.*, Application-Specific Integrated Circuit (ASIC), https://academy.binance.com/en/glossary/application-specific-integrated-circuit.

"The miners we operate are highly specialized computer servers built to use application-specific integrated circuit ("ASIC") chips that are designed specifically to mine bitcoin. With miners we produce computing power, known as "hash rate," with which we verify transactions on the Bitcoin blockchain. Bitcoin "mining" refers to the process of proposing and verifying transaction updates to the Bitcoin blockchain, which helps keep the Bitcoin network and its blockchain secure. Our bitcoin mining operation is focused on the generation of bitcoin by solving complex cryptographic algorithms to validate transactions on the Bitcoin network blockchain, which is commonly referred to as "mining."

See, *e.g.*, Core Scientific, Inc. Form 10-K, at 6, filed Feb. 27, 2025, available at https://investors.corescientific.com/sec-filings/all-sec-filings/content/0001628280-25-008302/0001628280-25-008302.pdf

Claim 1	CExemplary Evidence of Infringement

AUSTIN, Texas--(BUSINESS WIRE)-- **Core Scientific, Inc. (Nasdaq: CORZ)** ("Core Scientific" or "the Company"), a leader in digital infrastructure for high-performance computing and bitcoin mining, today released unaudited production and operations updates for January 2025.

Key Metrics Summary (unaudited)

Metric	January 2025	December 2024
Self-Mining Bitcoin Earned[1]	256	291
Hosting Bitcoin Earned by Customers[2]	17	18
Average Self-Mined Bitcoin Earned/Day	8.3	9.4
Self-Mining Energized Hash rate[3]	18.5	19.1
Hosting Energized Hash rate[4]	1.0	1.0
Total Energized Hash rate	19.5	20.1
Bitcoin Sold[5]	-	79
Bitcoin Sales Proceeds ($USD)	-	Appx. $7.7 million
Average Self-Mining Fleet Efficiency (J/TH)[6]	24.5	24.6

See, *e.g.*, https://investors.corescientific.com/news-events/press-releases/detail/106/core-scientific-announces-january-2025-production-and-operations-updates.

Core induces and/or contributes to the performance of this element by its customers, for example, by deploying and operating, for its customers, bitcoin mining machines that are not a staple article of commerce and are incapable of substantial noninfringing use. *See*, *e.g.*:

"Our Digital Asset Hosted Mining operation segment provides a full suite of services to our digital asset mining customers. We provide deployment, monitoring, troubleshooting, optimization and maintenance of our customers' digital asset mining equipment and provide necessary electrical power, repair and other infrastructure services necessary for our customers to operate, maintain and efficiently mine digital assets."

See, *e.g.*, Core Scientific, Inc. Form 10-K, at 7, filed Feb. 27, 2025, available at https://investors.corescientific.com/sec-filings/all-sec-filings/content/0001628280-25-008302/0001628280-25-008302.pdf

"The Company performs hosting services that enable customers to run blockchain and other high-performance computing operations."

Claim 1	CExemplary Evidence of Infringement
	See, *e.g.*, Core Scientific, Inc. Form 10-K, at 90, filed Feb. 27, 2025, available at https://investors.corescientific.com/sec-filings/all-sec-filings/content/0001628280-25-008302/0001628280-25-008302.pdf "As of December 31, 2024, [Core Scientific] had deployed … approximately 7,100 hosted miners, which represented … 1.0 EH/s." *Id*. at 8 *See*, *e.g.*, Core Scientific, Inc. Form 10-K, at 8, filed Feb. 27, 2025, available at https://investors.corescientific.com/sec-filings/all-sec-filings/content/0001628280-25-008302/0001628280-25-008302.pdf "Our hosting activities compete with a large number of other hosting operations. Our success in our hosting operations depends on our ability to supply hosting space and power, our performance with respect to installation, operation and repair of customer equipment, our ability to obtain replacement parts, the value of our service offering to our customers and the availability of mining equipment. To compete effectively as a hosting provider, we continue to market our services effectively to large-scale miners that value our ability to host at scale and who are willing to pay a premium hosting fee for our high up-time and operational expertise." *See*, *e.g.*, Core Scientific, Inc. Form 10-K, at 9, filed Feb. 27, 2025, available at https://investors.corescientific.com/sec-filings/all-sec-filings/content/0001628280-25-008302/0001628280-25-008302.pdf "We own and host specialized computers ('miners') configured for the purpose of validating transactions on multiple digital asset network blockchains (referred to as, 'mining'), predominantly the Bitcoin network. Substantially all of the miners we own and host were manufactured by Bitmain Technologies Limited ('Bitmain') and incorporate application-specific integrated circuit ('ASIC') chips specialized to solve blocks on the bitcoin blockchains using the 256-bit secure hashing algorithm ('SHA256') in return for bitcoin digital asset rewards." *See*, *e.g.*, Core Scientific, Inc. Form 10-K, at 48, filed Feb. 27, 2025, available at https://investors.corescientific.com/sec-filings/all-sec-filings/content/0001628280-25-008302/0001628280-25-008302.pdf

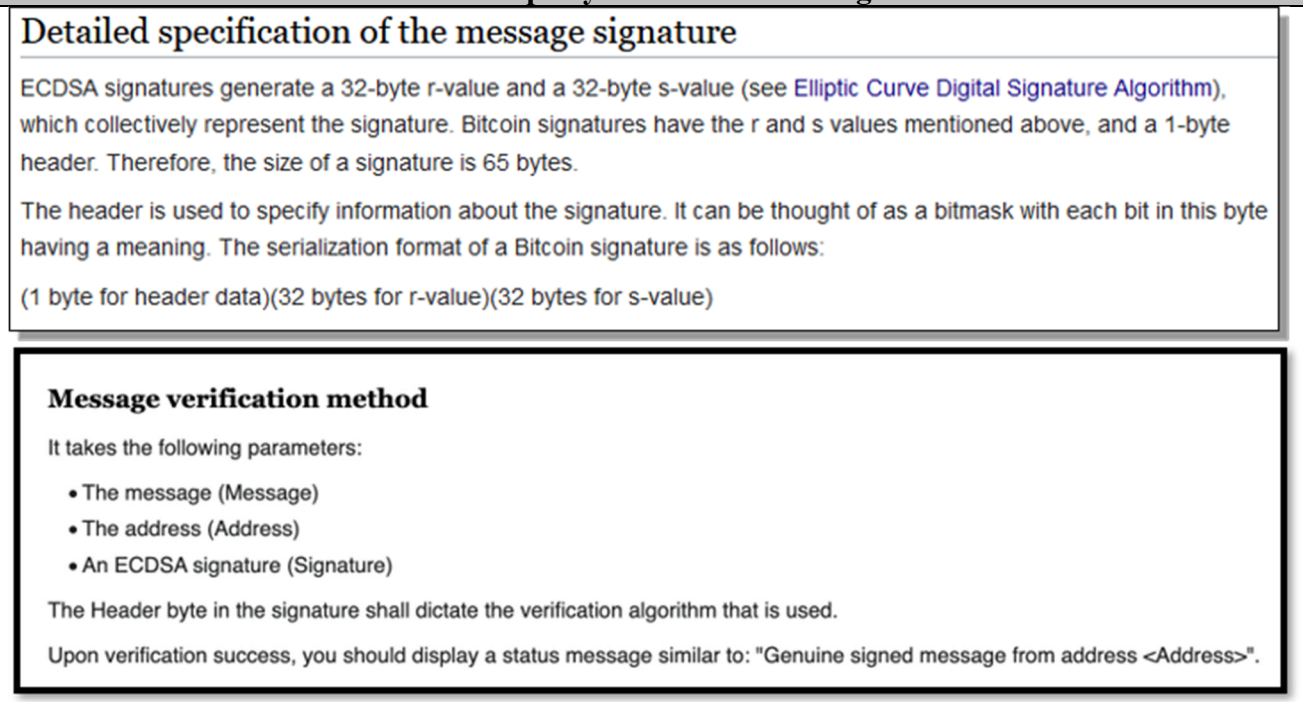
Claim 1	CExemplary Evidence of Infringement
1[a] receiving, by a receiver of the computing device and through a network, an electronic message including a signature, wherein the electronic message omits a public key of a signer, and the signature comprises a signature on the electronic message M;	Core receives, by a receiver of the computing device and through a network, an electronic message including a signature, wherein the electronic message omits a public key of a signer, and the signature comprises a signature on the electronic message M. For example, Core Scientific's miners receive, by a receiver of the computing device and through a network (*e.g.*, peer-to-peer network), an electronic message including a signature, wherein the electronic message omits a public key of a signer (*e.g.*, Bitcoin transferor), and the signature comprises a signature on the electronic message M. *See*, *e.g.*: The Signature is a base64-encoded ECDSA signature that, when decoded, with fields described in the next section. 3 Algorithm for signing and verifying messages 3.1 Definitions used in the algorithms 3.2 Constants 3.3 Message signing method 3.3.1 ECDSA signing, with P2PKH uncompressed addresses 3.3.2 ECDSA signing, with P2PKH compressed addresses 3.3.3 ECDSA signing, with P2WPKH-P2SH compressed addresses 3.3.4 ECDSA signing, with P2WPKH compressed addresses **Algorithm for signing and verifying messages** Below is a list of instructions for creating a BIP137-compliant message signing and verification algorithm. It is not required, but you should strip trailing newlines from the message before signing it, because some clients cannot process messages that contain trailing newlines. Below is a list of steps for signing and verifying a message, for each supported address type. *See*, *e.g.*, Message signing, https://en.bitcoin.it/wiki/Message_signing. "**Bitcoin signed messages have three parts, which are the Message, Address, and Signature**. The message is the actual message text - all kinds of text is supported, but it is recommended to avoid using

Claim 1	CExemplary Evidence of Infringement

	non-ASCII characters in the signature because they might be encoded in different character sets, preventing signature verification from succeeding.
	
	The address is a legacy, nested segwit, or native segwit address. Message signing from legacy addresses was added by Satoshi himself and therefore does not have a BIP. **Message signing from segwit addresses has been added by BIP137 … The Signature is a base64-encoded ECDSA signature** that, when decoded, with fields described in the next section." (Emphasis added)
	
	See, *e.g.,* Message Signing, https://en.bitcoin.it/wiki/Message_signing.
	
	"This document describes a signature format for **signing messages with Bitcoin private keys**.
	
	The specification is intended to describe the standard for signatures of messages that can be signed and verified between different clients that exist in the field today." (Emphasis added)
	
	See, *e.g.*, Bitcoin BIP137, https://github.com/bitcoin/bips/blob/master/bip-0137.mediawiki.
	
	For example, the electronic message includes a hash of the ECDSA public key instead of the public key itself. *See*, *e.g.*:
	
	Addresses
	A bitcoin address is in fact the hash of a ECDSA public key, computed this way:
	`Version = 1 byte of 0 (zero); on the test network, this is 1 byte of 111`
	`Key hash = Version concatenated with RIPEMD-160(SHA-256(public key))`
	`Checksum = 1st 4 bytes of SHA-256(SHA-256(Key hash))`
	`Bitcoin Address = Base58Encode(Key hash concatenated with Checksum)`
	
	See, *e.g.*, https://en.bitcoin.it/wiki/Protocol_documentation#Addresses.

Claim 1	CExemplary Evidence of Infringement
	Core induces and/or contributes to the performance of this element by its customers, for example, by deploying and operating, for its customers, bitcoin mining machines that are not a staple article of commerce and are incapable of substantial noninfringing use. *See*, *e.g.*: "Our Digital Asset Hosted Mining operation segment provides a full suite of services to our digital asset mining customers. We provide deployment, monitoring, troubleshooting, optimization and maintenance of our customers' digital asset mining equipment and provide necessary electrical power, repair and other infrastructure services necessary for our customers to operate, maintain and efficiently mine digital assets." *See*, *e.g.*, Core Scientific, Inc. Form 10-K, at 7, filed Feb. 27, 2025, available at https://investors.corescientific.com/sec-filings/all-sec-filings/content/0001628280-25-008302/0001628280-25-008302.pdf "The Company performs hosting services that enable customers to run blockchain and other high-performance computing operations." *See*, *e.g.*, Core Scientific, Inc. Form 10-K, at 90, filed Feb. 27, 2025, available at https://investors.corescientific.com/sec-filings/all-sec-filings/content/0001628280-25-008302/0001628280-25-008302.pdf "As of December 31, 2024, [Core Scientific] had deployed … approximately 7,100 hosted miners, which represented … 1.0 EH/s." *Id*. at 8 *See*, *e.g.*, Core Scientific, Inc. Form 10-K, at 8, filed Feb. 27, 2025, available at https://investors.corescientific.com/sec-filings/all-sec-filings/content/0001628280-25-008302/0001628280-25-008302.pdf "Our hosting activities compete with a large number of other hosting operations. Our success in our hosting operations depends on our ability to supply hosting space and power, our performance with respect to installation, operation and repair of customer equipment, our ability to obtain replacement parts, the value of our service offering to our customers and the availability of mining equipment. To compete effectively as a hosting provider, we continue to market our services effectively to large-scale miners that value our ability to host at scale and who are willing to pay a premium hosting fee for our high up-time and operational expertise."

Claim 1	CExemplary Evidence of Infringement
	See, *e.g.*, Core Scientific, Inc. Form 10-K, at 9, filed Feb. 27, 2025, available at https://investors.corescientific.com/sec-filings/all-sec-filings/content/0001628280-25-008302/0001628280-25-008302.pdf "We own and host specialized computers ('miners') configured for the purpose of validating transactions on multiple digital asset network blockchains (referred to as, 'mining'), predominantly the Bitcoin network. Substantially all of the miners we own and host were manufactured by Bitmain Technologies Limited ('Bitmain') and incorporate application-specific integrated circuit ('ASIC') chips specialized to solve blocks on the bitcoin blockchains using the 256-bit secure hashing algorithm ('SHA256') in return for bitcoin digital asset rewards." *See*, *e.g.*, Core Scientific, Inc. Form 10-K, at 48, filed Feb. 27, 2025, available at https://investors.corescientific.com/sec-filings/all-sec-filings/content/0001628280-25-008302/0001628280-25-008302.pdf
1[b] receiving, by the receiver of the computing device and through the network, a first elliptic curve point associated with a signature component from the signer, wherein the signature component comprises a first signature component r, the signature includes the first signature component r and a second signature component s, and the	Core receives, by the receiver of the computing device and through the network, a first elliptic curve point associated with a signature component from the signer, wherein the signature component comprises a first signature component r, the signature includes the first signature component r and a second signature component s, and the first elliptic curve point comprises an elliptic curve point R. For example, Core's miners receive a first elliptic curve point (*e.g.*, R) associated with a signature component (*e.g.*, r) from the signer, wherein the signature component comprises a first signature component r (*e.g.*, the r-value) and a second signature component s (*e.g.*, the s-value), and the first elliptic curve point comprises an elliptic curve point R. *See*, *e.g.*:

Claim 1	CExemplary Evidence of Infringement
first elliptic curve point comprises an elliptic curve point R;	 *See*, *e.g.*, Message signing, https://en.bitcoin.it/wiki/Message_signing. For example, Core's miners receive a first elliptic curve point (*e.g.*, R) associated with a signature component (*e.g.*, r) from the signer, wherein the signature component comprises a first signature component r (*e.g.*, the r-value) and a second signature component s (*e.g.*, the s-value), and the first elliptic curve point comprises an elliptic curve point R. For example, R=(x,y) where x=r or x=r+n. *See*, *e.g.*:

Claim 1	CExemplary Evidence of Infringement

ECDSA verification, P2WPKH compressed address

1. Set *r = DecodedSignature[1:33]*. If *r ≥ n* or *r == 0*, fail verification with an error similar to "Invalid ECDSA signature parameters".
2. Set *s = DecodedSignature[33:65]*. If *s ≥ n* or *s == 0*, fail verification with an error similar to "Invalid ECDSA signature parameters".
3. Set *z = SHA256(Message)*
4. Set *recID = Header AND 0x3*
5. If *recID AND 0x2 == 0*, set *x = r*, else set *x = r+n*.
6. Set *x = (x^3 + 7) mod p*
7. Set *y = x^((p+1)/4) mod p*
8. Calculate the correct parity of *y* using the 'recID':
   - If (*is_even(beta)* and *is_odd(recID)*) or (*is_odd(beta) and is_even(recID)*), set *y = p-y*.
9. Set *R = (x,y)*
10. Set *e = (-int(z)) % n*
11. Set *PublicKey = (R*s + G*e) * modinv(r, n)*
12. If *is_even(y)*, compute *EncodedPublicKey = "02" || hex(x)*. Else, compute *EncodedPublicKey = "03" || hex(x)*
13. Compute *AddressHash = RIPEMD160(SHA256(EncodedPublicKey)*
14. Compute *DerivedAddress = Bech32("bc", 0, AddressHash)*
15. If *DerivedAddress == Address*, succeed verification. Else fail verification with an error similar to "Wrong address for signature".

See, *e.g.*, Message signing, https://en.bitcoin.it/wiki/Message_signing.

Core induces and/or contributes to the performance of this element by its customers, for example, by deploying and operating, for its customers, bitcoin mining machines that are not a staple article of commerce and are incapable of substantial noninfringing use. *See*, *e.g.*:

"Our Digital Asset Hosted Mining operation segment provides a full suite of services to our digital asset mining customers. We provide deployment, monitoring, troubleshooting, optimization and maintenance of our customers' digital asset mining equipment and provide necessary electrical power, repair and other infrastructure services necessary for our customers to operate, maintain and efficiently mine digital assets."

See, *e.g.*, Core Scientific, Inc. Form 10-K, at 7, filed Feb. 27, 2025, available at https://investors.corescientific.com/sec-filings/all-sec-filings/content/0001628280-25-008302/0001628280-25-008302.pdf

Claim 1	CExemplary Evidence of Infringement
	"The Company performs hosting services that enable customers to run blockchain and other high-performance computing operations." *See*, *e.g.*, Core Scientific, Inc. Form 10-K, at 90, filed Feb. 27, 2025, available at https://investors.corescientific.com/sec-filings/all-sec-filings/content/0001628280-25-008302/0001628280-25-008302.pdf "As of December 31, 2024, [Core Scientific] had deployed … approximately 7,100 hosted miners, which represented … 1.0 EH/s." *Id*. at 8 *See*, *e.g.*, Core Scientific, Inc. Form 10-K, at 8, filed Feb. 27, 2025, available at https://investors.corescientific.com/sec-filings/all-sec-filings/content/0001628280-25-008302/0001628280-25-008302.pdf "Our hosting activities compete with a large number of other hosting operations. Our success in our hosting operations depends on our ability to supply hosting space and power, our performance with respect to installation, operation and repair of customer equipment, our ability to obtain replacement parts, the value of our service offering to our customers and the availability of mining equipment. To compete effectively as a hosting provider, we continue to market our services effectively to large-scale miners that value our ability to host at scale and who are willing to pay a premium hosting fee for our high up-time and operational expertise." *See*, *e.g.*, Core Scientific, Inc. Form 10-K, at 9, filed Feb. 27, 2025, available at https://investors.corescientific.com/sec-filings/all-sec-filings/content/0001628280-25-008302/0001628280-25-008302.pdf "We own and host specialized computers ('miners') configured for the purpose of validating transactions on multiple digital asset network blockchains (referred to as, 'mining'), predominantly the Bitcoin network. Substantially all of the miners we own and host were manufactured by Bitmain Technologies Limited ('Bitmain') and incorporate application-specific integrated circuit ('ASIC') chips specialized to solve blocks on the bitcoin blockchains using the 256-bit secure hashing algorithm ('SHA256') in return for bitcoin digital asset rewards."

Claim 1	CExemplary Evidence of Infringement
	See, *e.g.*, Core Scientific, Inc. Form 10-K, at 48, filed Feb. 27, 2025, available at https://investors.corescientific.com/sec-filings/all-sec-filings/content/0001628280-25-008302/0001628280-25-008302.pdf
1[c] recovering, by the hardware processor of the computing device, the omitted public key of the signer based on the received first elliptic curve point and the received signature, wherein the public key comprises a second elliptic curve point in an elliptic curve group different from the first elliptic curve point, wherein the elliptic curve group includes the first and second elliptic curve points, wherein the second elliptic curve point comprises an elliptic curve point Q, wherein recovering the omitted public key of the signer comprises computing Q=r−1 (sR−eG), wherein G comprises a generator of an elliptic	Core recovers, by the hardware processor of the computing device, the omitted public key of the signer based on the received first elliptic curve point and the received signature, wherein the public key comprises a second elliptic curve point in an elliptic curve group different from the first elliptic curve point, wherein the elliptic curve group includes the first and second elliptic curve points, wherein the second elliptic curve point comprises an elliptic curve point Q, wherein recovering the omitted public key of the signer comprises computing Q=r−1 (sR−eG), wherein G comprises a generator of an elliptic curve group that includes the elliptic curve point R and the elliptic curve point Q, and wherein e is a hash value computed from the electronic message M. For example, Core's miners recover the omitted public key (*e.g.*, PublicKey, Q) of the signer based on the received first elliptic curve point (*e.g.*, R) and the received signature (*e.g.*, (r,s)). *See*, *e.g.*:

Claim 1	CExemplary Evidence of Infringement
curve group that includes the elliptic curve point R and the elliptic curve point Q, and wherein e is a hash value computed from the electronic message M; and	**ECDSA verification, P2WPKH compressed address** 1. Set *r = DecodedSignature[1:33]*. If *r ≥ n* or *r == 0*, fail verification with an error similar to "Invalid ECDSA signature parameters". 2. Set *s = DecodedSignature[33:65]*. If *s ≥ n* or *s == 0*, fail verification with an error similar to "Invalid ECDSA signature parameters". 3. Set *z = SHA256(Message)* 4. Set *recID = Header AND 0x3* 5. If *recID AND 0x2 == 0*, set *x = r*, else set *x = r+n*. 6. Set *x = (x^3 + 7) mod p* 7. Set *y = x^((p+1)/4) mod p* 8. Calculate the correct parity of *y* using the 'recID': • If (*is_even(beta)* and *is_odd(recID)*) or (*is_odd(beta) and is_even(recID)*), set *y = p-y*. 9. Set *R = (x,y)* 10. Set *e = (-int(z)) % n* 11. Set *PublicKey = (R*s + G*e) * modinv(r, n)* 12. If *is_even(y)*, compute *EncodedPublicKey = "02" || hex(x)*. Else, compute *EncodedPublicKey = "03" || hex(x)* 13. Compute *AddressHash = RIPEMD160(SHA256(EncodedPublicKey)* 14. Compute *DerivedAddress = Bech32("bc", 0, AddressHash)* 15. If *DerivedAddress == Address*, succeed verification. Else fail verification with an error similar to "Wrong address for signature". *See*, *e.g.*, Message signing, https://en.bitcoin.it/wiki/Message_signing. The public key (*e.g.*, PublicKey) comprises a second elliptic curve point (*e.g.*, Q) in an elliptic curve group different from the first elliptic curve point (*e.g.*, R), wherein the elliptic curve group includes the first and second elliptic curve points. For example, points R and Q belong to the same elliptic curve group. *See*, *e.g.*:

Claim 1	CExemplary Evidence of Infringement

ECDSA verification, P2WPKH compressed address

1. Set *r = DecodedSignature[1:33]*. If *r ≥ n* or *r == 0*, fail verification with an error similar to "Invalid ECDSA signature parameters".
2. Set *s = DecodedSignature[33:65]*. If *s ≥ n* or *s == 0*, fail verification with an error similar to "Invalid ECDSA signature parameters".
3. Set *z = SHA256(Message)*
4. Set *recID = Header AND 0x3*
5. If *recID AND 0x2 == 0*, set *x = r*, else set *x = r+n*.
6. Set *x = (x^3 + 7) mod p*
7. Set *y = x^((p+1)/4) mod p*
8. Calculate the correct parity of *y* using the 'recID':
   - If (*is_even(beta)* and *is_odd(recID)*) or (*is_odd(beta) and is_even(recID)*), set *y = p-y*.
9. Set *R = (x,y)*
10. Set *e = (-int(z)) % n*
11. Set *PublicKey = (R*s + G*e) * modinv(r, n)*
12. If *is_even(y)*, compute *EncodedPublicKey = "02" || hex(x)*. Else, compute *EncodedPublicKey = "03" || hex(x)*
13. Compute *AddressHash = RIPEMD160(SHA256(EncodedPublicKey)*
14. Compute *DerivedAddress = Bech32("bc", 0, AddressHash)*
15. If *DerivedAddress == Address*, succeed verification. Else fail verification with an error similar to "Wrong address for signature".

See, *e.g.*, Message signing, https://en.bitcoin.it/wiki/Message_signing.

The second elliptic curve point comprises an elliptic curve point Q (*e.g.*, PublicKey), wherein recovering the omitted public key of the signer comprises computing Q=r−1 (sR−eG), wherein G comprises a generator of an elliptic curve group that includes the elliptic curve point R and the elliptic curve point Q, and wherein e is a hash value computed from the electronic message M. *See*, *e.g.*:

Claim 1	CExemplary Evidence of Infringement

ECDSA verification, P2WPKH compressed address

1. Set *r = DecodedSignature[1:33]*. If *r ≥ n* or *r == 0*, fail verification with an error similar to "Invalid ECDSA signature parameters".
2. Set *s = DecodedSignature[33:65]*. If *s ≥ n* or *s == 0*, fail verification with an error similar to "Invalid ECDSA signature parameters".
3. Set *z = SHA256(Message)*
4. Set *recID = Header AND 0x3*
5. If *recID AND 0x2 == 0*, set *x = r*, else set *x = r+n*.
6. Set *x = (x^3 + 7) mod p*
7. Set *y = x^((p+1)/4) mod p*
8. Calculate the correct parity of *y* using the 'recID':
   - If (*is_even(beta)* and *is_odd(recID)*) or (*is_odd(beta) and is_even(recID)*), set *y = p-y*.
9. Set *R = (x,y)*
10. Set *e = (-int(z)) % n*
11. Set *PublicKey = (R*s + G*e) * modinv(r, n)*
12. If *is_even(y)*, compute *EncodedPublicKey = "02" || hex(x)*. Else, compute *EncodedPublicKey = "03" || hex(x)*
13. Compute *AddressHash = RIPEMD160(SHA256(EncodedPublicKey)*
14. Compute *DerivedAddress = Bech32("bc", 0, AddressHash)*
15. If *DerivedAddress == Address*, succeed verification. Else fail verification with an error similar to "Wrong address for signature".

See, *e.g.*, Message signing, https://en.bitcoin.it/wiki/Message_signing.

The hash value e (*e.g.*, e) is computed from the message M using the formula e = (-int(z)) % n, where z is the hash value of the message (e.g., SHA256), as shown below.

Claim 1	CExemplary Evidence of Infringement

ECDSA verification, P2WPKH compressed address

1. Set *r = DecodedSignature[1:33]*. If *r ≥ n* or *r == 0*, fail verification with an error similar to "Invalid ECDSA signature parameters".
2. Set *s = DecodedSignature[33:65]*. If *s ≥ n* or *s == 0*, fail verification with an error similar to "Invalid ECDSA signature parameters".
3. Set *z = SHA256(Message)*
4. Set *recID = Header AND 0x3*
5. If *recID AND 0x2 == 0*, set *x = r*, else set *x = r+n*.
6. Set *x = (x^3 + 7) mod p*
7. Set *y = x^((p+1)/4) mod p*
8. Calculate the correct parity of *y* using the 'recID':
   - If (*is_even(beta)* and *is_odd(recID)*) or (*is_odd(beta) and is_even(recID)*), set *y = p-y*.
9. Set *R = (x,y)*
10. Set *e = (-int(z)) % n*
11. Set *PublicKey = (R*s + G*e) * modinv(r, n)*
12. If *is_even(y)*, compute *EncodedPublicKey = "02" || hex(x)*. Else, compute *EncodedPublicKey = "03" || hex(x)*
13. Compute *AddressHash = RIPEMD160(SHA256(EncodedPublicKey)*
14. Compute *DerivedAddress = Bech32("bc", 0, AddressHash)*
15. If *DerivedAddress == Address*, succeed verification. Else fail verification with an error similar to "Wrong address for signature".

See, *e.g.*, Message signing, https://en.bitcoin.it/wiki/Message_signing.

The elliptic curve point comprises a first elliptic curve point R, the public key of the signer comprises a second elliptic curve point Q, and generating the public key of the signer comprises computing Q=r−1 (sR−eG), and G comprises a generator of an elliptic curve group that includes the first elliptic curve point R and the second elliptic curve point Q. The above equation is used to determine Q, which is the PublicKey (a point on the elliptic curve secp256k1). *See*, *e.g.*:

Constants

The constant *Inf* shall refer to the point at infinity, of the secp256k1 curve.

The constant *p* shall refer to the secp256k1 field size, aka. curve characteristic, defined as *int(FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE FFFFFC2F)*

The constant *n* shall refer to the secp256k1 curve order, defined as *int(FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE BAAEDCE6 AF48A03B BFD25E8C D0364141)*

The constant *G* shall refer to the secp256k1 generator point, defined as *(79BE667E F9DCBBAC 55A06295 CE870B07 029BFCDB 2DCE28D9 59F2815B 16F81798, 483ADA77 26A3C465 5DA4FBFC 0E1108A8 FD17B448 A6855419 9C47D08F FB10D4B8)*

Claim 1	CExemplary Evidence of Infringement
	See, *e.g.*, Message signing, https://en.bitcoin.it/wiki/Message_signing. Core induces and/or contributes to the performance of this element by its customers, for example, by deploying and operating, for its customers, bitcoin mining machines that are not a staple article of commerce and are incapable of substantial noninfringing use. *See*, *e.g.*: "Our Digital Asset Hosted Mining operation segment provides a full suite of services to our digital asset mining customers. We provide deployment, monitoring, troubleshooting, optimization and maintenance of our customers' digital asset mining equipment and provide necessary electrical power, repair and other infrastructure services necessary for our customers to operate, maintain and efficiently mine digital assets." *See*, *e.g.*, Core Scientific, Inc. Form 10-K, at 7, filed Feb. 27, 2025, available at https://investors.corescientific.com/sec-filings/all-sec-filings/content/0001628280-25-008302/0001628280-25-008302.pdf "The Company performs hosting services that enable customers to run blockchain and other high-performance computing operations." *See*, *e.g.*, Core Scientific, Inc. Form 10-K, at 90, filed Feb. 27, 2025, available at https://investors.corescientific.com/sec-filings/all-sec-filings/content/0001628280-25-008302/0001628280-25-008302.pdf "As of December 31, 2024, [Core Scientific] had deployed … approximately 7,100 hosted miners, which represented … 1.0 EH/s." *Id*. at 8 *See*, *e.g.*, Core Scientific, Inc. Form 10-K, at 8, filed Feb. 27, 2025, available at https://investors.corescientific.com/sec-filings/all-sec-filings/content/0001628280-25-008302/0001628280-25-008302.pdf "Our hosting activities compete with a large number of other hosting operations. Our success in our hosting operations depends on our ability to supply hosting space and power, our performance with respect to installation, operation and repair of customer equipment, our ability to obtain replacement parts, the value of our service offering to our customers and the availability of mining equipment. To compete effectively as a hosting provider, we continue to market our services effectively to large-scale

Claim 1	CExemplary Evidence of Infringement
	miners that value our ability to host at scale and who are willing to pay a premium hosting fee for our high up-time and operational expertise." *See*, *e.g.*, Core Scientific, Inc. Form 10-K, at 9, filed Feb. 27, 2025, available at https://investors.corescientific.com/sec-filings/all-sec-filings/content/0001628280-25-008302/0001628280-25-008302.pdf "We own and host specialized computers ('miners') configured for the purpose of validating transactions on multiple digital asset network blockchains (referred to as, 'mining'), predominantly the Bitcoin network. Substantially all of the miners we own and host were manufactured by Bitmain Technologies Limited ('Bitmain') and incorporate application-specific integrated circuit ('ASIC') chips specialized to solve blocks on the bitcoin blockchains using the 256-bit secure hashing algorithm ('SHA256') in return for bitcoin digital asset rewards." *See*, *e.g.*, Core Scientific, Inc. Form 10-K, at 48, filed Feb. 27, 2025, available at https://investors.corescientific.com/sec-filings/all-sec-filings/content/0001628280-25-008302/0001628280-25-008302.pdf
1[d] verifying, by the hardware processor of the computing device, the received signature using the recovered public key which provides an accelerated verification of the received signature.	Core verifies, by the hardware processor of the computing device, the received signature using the recovered public key which provides an accelerated verification of the received signature. For example, Core's miners verify that the second elliptic curve point Q represents the public key of the signer. *See*, *e.g.*:

Claim 1	CExemplary Evidence of Infringement

ECDSA verification, P2WPKH compressed address

1. Set *r = DecodedSignature[1:33]*. If *r ≥ n* or *r == 0*, fail verification with an error similar to "Invalid ECDSA signature parameters".
2. Set *s = DecodedSignature[33:65]*. If *s ≥ n* or *s == 0*, fail verification with an error similar to "Invalid ECDSA signature parameters".
3. Set *z = SHA256(Message)*
4. Set *recID = Header AND 0x3*
5. If *recID AND 0x2 == 0*, set *x = r*, else set *x = r+n*.
6. Set *x = (x^3 + 7) mod p*
7. Set *y = x^((p+1)/4) mod p*
8. Calculate the correct parity of *y* using the 'recID':
   - If (*is_even(beta)* and *is_odd(recID)*) or (*is_odd(beta) and is_even(recID)*), set *y = p-y*.
9. Set *R = (x,y)*
10. Set *e = (-int(z)) % n*
11. Set *PublicKey = (R*s + G*e) * modinv(r, n)*
12. If *is_even(y)*, compute *EncodedPublicKey = "02" || hex(x)*. Else, compute *EncodedPublicKey = "03" || hex(x)*
13. Compute *AddressHash = RIPEMD160(SHA256(EncodedPublicKey)*
14. Compute *DerivedAddress = Bech32("bc", 0, AddressHash)*
15. If *DerivedAddress == Address*, succeed verification. Else fail verification with an error similar to "Wrong address for signature".

See, *e.g.*, Message signing, https://en.bitcoin.it/wiki/Message_signing.

Core induces and/or contributes to the performance of this element by its customers, for example, by deploying and operating, for its customers, bitcoin mining machines that are not a staple article of commerce and are incapable of substantial noninfringing use. *See*, *e.g.*:

"Our Digital Asset Hosted Mining operation segment provides a full suite of services to our digital asset mining customers. We provide deployment, monitoring, troubleshooting, optimization and maintenance of our customers' digital asset mining equipment and provide necessary electrical power, repair and other infrastructure services necessary for our customers to operate, maintain and efficiently mine digital assets."

See, *e.g.*, Core Scientific, Inc. Form 10-K, at 7, filed Feb. 27, 2025, available at https://investors.corescientific.com/sec-filings/all-sec-filings/content/0001628280-25-008302/0001628280-25-008302.pdf

Claim 1	CExemplary Evidence of Infringement
	"The Company performs hosting services that enable customers to run blockchain and other high-performance computing operations." *See*, *e.g.*, Core Scientific, Inc. Form 10-K, at 90, filed Feb. 27, 2025, available at https://investors.corescientific.com/sec-filings/all-sec-filings/content/0001628280-25-008302/0001628280-25-008302.pdf "As of December 31, 2024, [Core Scientific] had deployed … approximately 7,100 hosted miners, which represented … 1.0 EH/s." *Id*. at 8 *See*, *e.g.*, Core Scientific, Inc. Form 10-K, at 8, filed Feb. 27, 2025, available at https://investors.corescientific.com/sec-filings/all-sec-filings/content/0001628280-25-008302/0001628280-25-008302.pdf "Our hosting activities compete with a large number of other hosting operations. Our success in our hosting operations depends on our ability to supply hosting space and power, our performance with respect to installation, operation and repair of customer equipment, our ability to obtain replacement parts, the value of our service offering to our customers and the availability of mining equipment. To compete effectively as a hosting provider, we continue to market our services effectively to large-scale miners that value our ability to host at scale and who are willing to pay a premium hosting fee for our high up-time and operational expertise." *See*, *e.g.*, Core Scientific, Inc. Form 10-K, at 9, filed Feb. 27, 2025, available at https://investors.corescientific.com/sec-filings/all-sec-filings/content/0001628280-25-008302/0001628280-25-008302.pdf "We own and host specialized computers ('miners') configured for the purpose of validating transactions on multiple digital asset network blockchains (referred to as, 'mining'), predominantly the Bitcoin network. Substantially all of the miners we own and host were manufactured by Bitmain Technologies Limited ('Bitmain') and incorporate application-specific integrated circuit ('ASIC') chips specialized to solve blocks on the bitcoin blockchains using the 256-bit secure hashing algorithm ('SHA256') in return for bitcoin digital asset rewards."

Claim 1	CExemplary Evidence of Infringement
	See, *e.g.*, Core Scientific, Inc. Form 10-K, at 48, filed Feb. 27, 2025, available at https://investors.corescientific.com/sec-filings/all-sec-filings/content/0001628280-25-008302/0001628280-25-008302.pdf